Defense Information Systems Agency
Center for Standards

DEPARTMENT OF DEFENSE TECHNICAL ARCHITECTURE FRAMEWORK FOR INFORMATION MANAGEMENT

Volume 2: Technical Reference Model

Version 3.0

30 April 1996

DRAFT SF 298

1. Report Date (dd-mm-yy) 30 April 1996	2. Report Type	3. Dates covered (from... to)
4. Title & subtitle Department of Defense Technical Architecture Framework for Information Management. Volume 2: Technical Reference Model. Version 3.0		5a. Contract or Grant # 5b. Program Element #
6. Author(s)		5c. Project # 5d. Task # 5e. Work Unit #
7. Performing Organization Name & Address		8. Performing Organization Report #
9. Sponsoring/Monitoring Agency Name & Address Defense Information Systems Agency Center for Standards 10701 Parkridge Blvd Reston, VA 20191		10. Monitor Acronym 11. Monitor Report #
12. Distribution/Availability Statement Approved for Public Release: Distribution is Unlimited		
13. Supplementary Notes		
14. Abstract 		
15. Subject Terms		

16. Report Unclass	17. Abstract Unclass	18. This Page Unclass	19. Limitation of Abstract	20. # of Pages	21. Responsible Person (Name and Telephone #) Marilyn McLaughlin (703) 735-3563

FOREWORD:
ABOUT THIS DOCUMENT

This edition of the Technical Architecture Framework for Information Management (TAFIM) replaces Version 2.0, dated 30 June 1994. Version 3.0 comprises eight volumes, as listed on the following configuration management page.

TAFIM HARMONIZATION AND ALIGNMENT

- This TAFIM version is the result of a review and comment coordination period that began with the release of the 30 September 1995 Version 3.0 Draft. During this coordination period, a number of extremely significant activities were initiated by DoD. As a result, the version of the TAFIM that was valid at the beginning of the coordination period is now "out of step" with the direction and preliminary outcomes of these DoD activities. Work on a complete TAFIM update is underway to reflect the policy, guidance, and recommendations coming from theses activities as they near completion. Each TAFIM volume will be released as it is updated. Specifically, the next TAFIM release will fully reflect decisions stemming from the following:

- The DoD 5000 Series of acquisition policy and procedure documents

- The Joint Technical Architecture (JTA), currently a preliminary draft document under review.

- The C4ISR Integrated Task Force (ITF) recommendations on Operational, Systems, and Technical architectures.

SUMMARY OF MAJOR CHANGES AND EXPECTED UPDATES

This document, Volume 2 of the TAFIM, contains significant revisions from the Version 2.0 edition of this volume. These changes are the result of a harmonization of Volumes 2, 4, and 7 conducted by MITRE for the Defense Information Systems Agency (DISA) Joint Interoperability and Engineering Organization (JIEO) Center for Standards (CFS). All of the proposed harmonization changes could not be implemented at this time because of the time and resources available and the level of consensus within the Architecture Methodology Working Group (AMWG). Volume 2 has been updated with those changes that could be accomplished within the time available. The major changes to Volume 2 are as follows:

- Removed all references to specific standards from Volume 2, in accordance with the status of Volume 7 as the definitive repository of standards data.

- Defined the terms Major Service Area (MSA), Mid-Level Service Area (MLSA), and Base Service Area (BSA).

- Harmonized the MLSAs and BSAs in Volume 7 with those in Volume 2, and incorporated the Volume 7 MLSA and BSA definitions into the Volume 2 definitions. In addition, certain MLSA definitions in Volume 2 that were not harmonized were adjusted to mirror the definitions of the MLSAs and BSAs in Volume 7.

- Modified the Technical Reference Model (TRM) shown in Figure 2-2 to depict the MLSAs that were in Volume 7 and are now incorporated in Volume 2, and identified that part of the model that contains the MSAs and MLSAs.

In addition, changes have been made to bring the guidance provided in this volume more in line with current policies. Work remains to be done to fully reflect the impact of the policy documents and decisions noted above; this edition of the TAFIM has been released to serve as a baseline and to make available throughout the DoD community the additions and modifications that have been implemented to date.

A historical perspective on the development of this volume and its changes over time appears in the Preface.

A NOTE ON VERSION NUMBERING

A version numbering scheme approved by the AMWG will control the version numbers applied to all future editions of TAFIM volumes. Version numbers will be applied and incremented as follows:

- This edition of the TAFIM is designated as the official Version 3.0.

- From this point forward, single volumes will be updated and republished as needed. The second digit in the version number will be incremented each time (e.g., Volume 7 Version 3.1). The new version number will be applied only to the volume(s) that are updated at that time. There is no limit to the number of times the second digit can be changed to account for new editions of particular volumes.

- On an infrequent basis (e.g., every two years or more), the entire TAFIM set will be republished at once. Only when all volumes are released simultaneously will the first digit in the version number be changed. The next complete version will be designated Version 4.0.

- TAFIM volumes bearing a two-digit version number (e.g., Version 3.0, 3.1, etc.) without the DRAFT designation are final, official versions of the TAFIM. Only the TAFIM program manager can change the two-digit version number on a volume.

- A third digit can be added to the version number as needed to control working drafts, proposed volumes, internal review drafts, and other unofficial releases. The sponsoring organization can append and change this digit as desired.

Certain TAFIM volumes developed for purposes outside the TAFIM may appear under a different title and with a different version number from those specified in the configuration management page. These editions are not official releases of TAFIM volumes.

DISTRIBUTION

Version 3.0 is available for download from the DISA Information Technology Standards Information (ITSI) bulletin board system (BBS). Users are welcome to add the TAFIM files to individual organizations' BBSs or file servers to facilitate wider availability.

This final release of Version 3.0 will be made available on the World Wide Web shortly after hard-copy publication. DISA is investigating other electronic distribution approaches to facilitate access to the TAFIM and to enhance its usability.

This page intentionally left blank.

TAFIM Document Configuration Management Page

The latest **authorized versions of the TAFIM** volumes are as follows:

Volume 1: Overview	3.0	30 April 1996
Volume 2: Technical Reference Model	3.0	30 April 1996
Volume 3: Architecture Concepts & Design Guidance	3.0	30 April 1996
Volume 4: DoD SBA Planning Guide	3.0	30 April 1996
Volume 5: Program Manager's Guide for Open Systems	3.0	30 April 1996
Volume 6: DoD Goal Security Architecture	3.0	30 April 1996
Volume 7: Adopted Information Technology Standards	3.0	30 April 1996
Volume 8: HCI Style Guide	3.0	30 April 1996

Working drafts may have been released by volume sponsors for internal coordination purposes. It is not necessary for the general reader to obtain and incorporate these unofficial, working drafts.

Note: Only those versions listed above as authorized versions represent official editions of the TAFIM.

This page intentionally left blank.

PREFACE

The first draft of the Corporate Information Management (CIM) Technical Reference Model was submitted to DoD components for review on 4 September 1991. The review resulted in a number of editorial and minor technical changes that were included in Version 1.0 of the document. Additional comments and issues received as a result of staffing Version 1.0 resulted in the development of Version 1.1 of the document. Version 1.1 was submitted to the Information Technology Policy Board (ITPB) for approval in December 1991. On 12 February 1992, the Director of Defense Information (DDI) approved the use of Version 1.1 of the CIM Technical Reference Model by all DoD components. Version 1.1 was circulated widely within DoD and submitted to industry and other government activities for review. On 25 August 1992, the DDI approved the use of Version 1.2 of the Technical Reference Model.

The foremost issue identified during the review of the draft CIM Technical Reference Model was the extent to which future editions would expand to conform to either the National Institute of Standards and Technology (NIST) Application Portability Profile (APP) or emerging reference models based on the work of the Institute of Electrical and Electronics Engineers (IEEE), Open Software Foundation (OSF), UNIX International (UI), International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)/Joint Technical Committee 1 (JTC1), X/Open Limited, Accredited Standards Committee (ASC), and other national/international activities. The DISA JIEO staff continues to consult extensively with NIST and other external organizations on this issue.

The first major change to the CIM Technical Reference Model was the addition of the draft NIST FIPS Publication on the Government Network Management Profile (GNMP) that was added to the CIM standards profile as part of Version 1.1. Certain military features not yet contained in the draft GNMP Federal Information Processing Standard (FIPS) were to be documented in MIL-STD-2045-38000, Network Management for DoD Communications, and forwarded to NIST for incorporation in future versions of the FIPS. The recommendation to include the Draft GNMP FIPS and associated Military Standard was approved by the Architecture Methodology Working Group.

Version 1.2, known as the Technical Reference Model for Information Management, was published in May 1992. Version 1.2 included FIPS Publication 161 (Electronic Data Interchange), a limited discussion of Ada bindings, and a requirement for standards conformance testing. In addition, the figures in Version 1.2 were modified slightly in response to a number of vendor and DoD comments. Version 1.2 also contained a detailed discussion on security services and standards.

Version 1.3 of the Technical Reference Model was published in December 1992 and incorporated as Volume 3 of the Technical Architecture Framework for Information Management (TAFIM). Version 1.3 provided the necessary changes for closer alignment of the Technical Reference Model with the IEEE POSIX 1003.0 Draft Guide. Also included in Version 1.3 were the results of the harmonization of the Technical Reference Model and the

Computer-aided Acquisition and Logistics Support (CALS) architecture. Additional CALS standards, such as raster graphics, and an expanded discussion about each standard, to include up-to-date document references, were provided. In addition, several vendor comments submitted during the review of Version 1.1 were addressed.

Version 2.0 of the Technical Reference Model addressed several additional important topics. This version included the services and standards needed to support DoD's distributed computing requirements. In addition, requirements for internationalization services resulting from harmonization of the Technical Reference Model with North Atlantic Treaty Organization (NATO) reference model development efforts were addressed. Further, a new objective was added and the security material was significantly supplemented throughout the document to reflect the integration of the DoD Goal Security Architecture into the TAFIM domain. This version also reflected agreements reached between the DISA Center for Architecture and the DISA Center for Standards to incorporate the DoD Profile of Standards, which is the Adopted Information Technology Standards, (AITS) in a separate TAFIM volume, Volume 7. The DoD Profile of Standards or AITS, which corresponds to the reference model services and interfaces, is described in detail in Volume 7.

Areas to be addressed in future versions of Volume 2 include services and standards for tactical systems, imagery, and multimedia data transfer. A set of metrics, based on the NIST APP, will be provided to assist users in choosing extensions to the current standards in those areas where standards do not exist, or where consensus has not been achieved. Features and services required by the Communication-Electronics Accommodation Program (CAP) in support of handicapped access to DoD computer resources will also be added.

Version 3.0 of the Technical Reference Model addresses the harmonization of Volumes 2 and 7. In addition, the definitions of MSAs, MLSAs, and BSAs have been included in Volume 2. Further, Version 3.0 harmonized the MLSA and BSAs in Volume 7 with those Volume 2 and incorporated the Volume 7 MLSA definitions into Volume 2. The Technical Reference Model graphic was modified to depict the new MLSAs from Volume 7.

CONTENTS

FIGURES

This page intentionally left blank.

1.0 INTRODUCTION

1.1 BACKGROUND

On 16 November 1990, the Secretary of Defense directed the implementation of the Department of Defense (DoD) Corporate Information Management (CIM) initiative, hereafter known as the DoD Information Management initiative, to strengthen the DoD's ability to apply computing, telecommunications, and information management capabilities effectively in the accomplishment of the DoD mission. Transition of the DoD's present information systems and associated information technology resources to a communications and computing infrastructure based on the principles of open systems architecture and systems transparency is a key strategy for implementing the Department's Information Management initiative. The development of a technical reference model and the selection of associated standards are first steps toward executing this strategy.

1.2 PURPOSE AND OBJECTIVES

The purpose of the Technical Reference Model described in this document is to provide a common conceptual framework, and define a common vocabulary so that the diverse components within the DoD can better coordinate acquisition, development, and support of DoD information systems. The Technical Reference Model also provides a high-level representation of the information system domain showing major service areas. DoD Components are required to apply the model to increase commonality and interoperability across the DoD, as directed by the Director of Defense Information (DDI) Policy Memorandum of 12 February 1992, Subject: Open Systems Implementation and the Technical Reference Model. On 25 August 1992, the DDI approved the use of the first update to the Technical Reference Model for Information Management (Version 1.2) (see Appendix C).

The model is not a specific system architecture. Rather, it establishes a common vocabulary and defines a set of services and interfaces common to DoD information systems. The reference model and standards profile define the target technical environment for the acquisition, development, and support of DoD information systems.

The objectives to be achieved through application of the technical reference model presented in this document are as follows:

- Improve user productivity
- Improve development efficiency
- Improve portability and scalability
- Improve interoperability
- Promote vendor independence

- Reduce life-cycle costs
- Improve security
- Improve manageability.

1.3 STANDARDIZATION EFFORTS

NIST is currently pursuing the definition of an Open System Environment (OSE), which encompasses the functionality needed to provide interoperability, portability, and scalability of computerized applications across networks of heterogeneous hardware/software platforms. In April 1991, NIST published the first version of the Application Portability Profile (APP), which defines a reference model and outlines a suite of selected specifications (i.e., standards) that define the interfaces, services, protocols, and data formats for implementation of OSE within the U.S. Government. In June 1993, NIST published Version 2.0 of the APP as NIST Special Publication 500-210. The Technical Reference Model is adapted from the NIST model to meet the requirements of DoD and conforms to NIST recommendations wherever possible. As NIST continues to evolve the APP, changes will be considered for incorporation into the Technical Reference Model. As DoD requirements evolve, proposed changes to the APP will be forwarded to NIST. DISA will continue to work with NIST and other national and international standards organizations to ensure that the NIST APP and emerging standards meet or are compatible with the needs of DoD.

1.4 APPROACH

Major DoD component documents, including the DoD Intelligence Information System (DODIIS) Reference Model, were analyzed using the NIST APP as a baseline to derive the Technical Reference Model. The maturity, stability, completeness, and availability of standards for the service areas defined in the Technical Reference Model were then assessed. Where adequate standards were not available or multiple conflicting standards were contending for consensus, an issue was identified and an action plan was established.

The Technical Reference Model does not represent a final position, but is an evolutionary target. As technology continues to advance and additional standards emerge, the Architecture Methodology Working Group will continue to update the standards profile and recommend refinements in the Reference Model to the Office of the Secretary of Defense (OSD).

1.5 DOCUMENT ORGANIZATION

The Technical Reference Model document consists of two sections and four appendices. Section 2 provides an overview of the Technical Reference Model, the principles upon which the model is based, and the services to be provided. References and acronyms are identified in Appendices A and B, respectively. Appendix C contains the DDI memoranda dated 12 February 1992 and 25 August 1992 concerning the Technical Reference Model. Appendix D contains instructions and a template for commenting on this document.

2.0 DOD TECHNICAL REFERENCE MODEL

2.1 OVERVIEW

Within the context of information systems, a reference model is defined to be a generally accepted representation that allows people to agree on definitions, build common understanding, and identify issues for resolution. A technical reference model is necessary to establish a context for understanding how the disparate technologies required to implement information management relate to each other. The model also provides a mechanism for identifying the key issues associated with applications portability, scalability, and interoperability. The Technical Reference Model is not a specific system design. Rather, it establishes a common vocabulary and defines a set of services and interfaces common to DoD information systems. The Technical Reference Model will serve to facilitate interoperability between mission-area applications, portability across mission areas, and cost reductions through the use of common services. The development and acceptance of the Technical Reference Model is critical to the successful implementation of the DoD Information Management initiative.

2.2 PRINCIPLES

The Technical Reference Model was devised to permit the DoD to take advantage of the benefits of open systems and the new technologies available in the commercial market. DoD-wide application of the model should result in cost savings over the long term. Section 1 outlined the Technical Reference Model objectives. The principles that support these objectives and that will be used to refine and implement the Reference Model are described below.

OBJECTIVE 1: IMPROVE USER PRODUCTIVITY

User productivity improvements will be realized by applying the following principles:

- **Consistent User Interface.** A consistent user interface will ensure that all user accessible functions and services will appear and behave in a similar, predictable fashion regardless of application or site. This has the benefits of simplifying training, facilitating the development of future applications, improving ease of use across applications, and promoting application portability.

- **Integrated Applications.** Applications available to the user will behave in a logically consistent manner across user environments. Support applications, such as office automation and electronic mail, will be used as an integrated set with mission area specific applications.

- **Data Sharing.** Databases will be shared across DoD in the context of security and operational considerations. Concepts and tools that promote data sharing include adherence to standard database development rules, the use of DoD data dictionary and software reuse libraries, and strong DoD commitment to resource sharing.

OBJECTIVE 2: IMPROVE DEVELOPMENT EFFICIENCY

The efficiency of development efforts will be improved by applying the following principles:

- **Common Development.** Applications that are common to multiple mission areas will be centrally developed or acquired.

- **Common Open Systems Environment.** A standards-based common operating environment, which accommodates the injection of new standards, technologies, and applications on a DoD-wide basis, will be established. This standards-based environment will provide the basis for development of common applications and facilitate software reuse.

- **Use of Products.** To the extent possible, hardware-independent, nondevelopmental items (NDI) should be used to satisfy requirements in order to reduce the dependence on custom developments and to reduce development and maintenance costs.

- **Software Reuse.** For those applications that must be custom developed, incorporating software reuse into the development methodology will reduce the amount of software developed and add to the inventory of software suitable for reuse by other systems.

- **Resource Sharing.** Data processing resources (hardware, software, and data) will be shared by all users requiring the services of those resources. Resource sharing will be accomplished in the context of security and operational considerations.

OBJECTIVE 3: IMPROVE PORTABILITY AND SCALABILITY

The portability and scalability of applications will be improved by applying the following principles:

- **Portability.** Applications that implement the model's paradigms will be portable, allowing for movement across heterogeneous computing platforms with minimal or no modifications. With portable applications, implementing activities will be able to upgrade their hardware base as technological improvements occur, with minimal impact on operations.

- **Scalability.** Applications that conform to the model will be configurable, allowing operation on the full spectrum of platforms depending on user requirements.

OBJECTIVE 4: IMPROVE INTEROPERABILITY

Interoperability improvements across applications and mission areas can be realized by applying the following principles:

- **Common Infrastructure**. The DoD will develop and implement a communications and computing infrastructure based on open systems and systems transparency including, but not limited to, operating systems, database management, data interchange, network services,

network management, and user interfaces. The basis for common infrastructure is to identify core capabilities having a commonality of application across services. This, in the near term, enables the migration from static and monolithic applications (stovepipes) to a more open environment enabling data and data format transparency across heterogeneous platforms.

- **Standardization.** By implementing standards from the DoD Profile of Standards (see Section 3), applications will be provided and will be able to use a common set of services that improve the opportunities for interoperability.

OBJECTIVE 5: PROMOTE VENDOR INDEPENDENCE

Vendor independence will be promoted by applying the following principles:

- **Interchangeable Components.** Hardware and software supporting or migrating to open systems compliance will be acquired or implemented, so that upgrades or the insertion of new products will result in minimal disruption to the user's environment.

- **Non-Proprietary Specifications.** Capabilities will be defined in terms of non-proprietary specifications that support full and open competition and are available to any vendor for use in developing commercial products.

OBJECTIVE 6: REDUCE LIFE-CYCLE COSTS

Life-cycle costs can be reduced by applying most of the principles discussed above. In addition, the following principles directly address reducing life-cycle costs:

- **Reduced Duplication.** Replacement of "stovepipe" systems and "islands of automation" with interconnected open systems, which can share data and other resources, will dramatically reduce overlapping functionality, data duplication, and unneeded redundancy.

- **Reduced Software Maintenance Costs.** Software complexity may increase with increased user demand for services such as distributed processing and distributed database services. However, if the principles described above are implemented, reductions in software maintenance will be realized because there will be less software to maintain. In those cases where the number of DoD users is small, increased use of standard nondevelopmental software will further reduce costs since vendors of such software distribute their product maintenance costs across a much larger user base.

- **Reduced Training Costs.** A reduction in training costs will be realized because users rotating to new organizations will already be familiar with the common systems and consistent human computer interfaces (HCI).

OBJECTIVE 7: IMPROVE SECURITY

Security will be improved in DoD information systems by satisfaction of the following principles for information systems that may need to operate simultaneously in various DoD environments (tactical, strategic, and sustaining base):

- **Uniform Security Accreditation and Certification.** Uniform certification and accreditation procedures will not only reduce the time needed to approve system operation but will result in more consistent use of security mechanisms to protect sensitive data.

- **Consistent Security Interfaces.** Consistent security interfaces and labeling procedures will reduce errors when managing sensitive data and reduce learning time when changing from system to system. Not all mission-area applications will need the same suite of security features, but any features used will be consistent across applications. Users will see the same security labels in a common format and manage them in the same way.

- **Support for Simultaneous Processing in Single Platforms of Different Information Domains.** Security protection will be provided for simultaneous processing of various categories of information within a single system. Information systems that can support multiple security policies can support multiple missions with varying sensitivity and rules for protected use. This will include support of simultaneous processing under multiple security policies of any complexity or type, including policies for sensitive unclassified information and multiple categories of classified information. This type of support will also permit users with different security attributes to simultaneously use the system. Separate or dedicated information systems for processing information controlled by different security policies will be reduced or eliminated.

- **Support for Simultaneous Processing in a Distributed System of Different Information Domains.** Security protection will be provided for simultaneous processing of various categories of information in a distributed environment. This protection will apply to processing of information controlled by multiple security policies in distributed networks using heterogeneous platforms and communications networks. This will greatly extend the flexibility of the system implementor in providing cost-effective information systems based on open systems principles.

- **Support for Use of Common User Communications Systems.** Security protection will be provided in such a way as to permit use of common carrier (public) systems for communications connectivity. It will also permit the use of Department-owned common user communications systems. This use of public and Department common user global communications networks will result in the potential for enhanced cost effective interoperability across mission areas.

OBJECTIVE 8: IMPROVE MANAGEABILITY

Management improvement can be realized by applying the following principles:

- **Consistent Management Interface.** Consistency of management practices and procedures will facilitate management across all applications and their underlying support structures. Users will accomplish work more efficiently by having the management burden simplified through such an interface.

- **Management Standardization.** By standardizing management practices, control of individual and consolidated processes will be improved in all interoperable scenarios.

- **Reduced Operation, Administration, and Maintenance (OA&M) Costs.** OA&M costs will be reduced through the availability of improved management products and increased standardization of objects being managed.

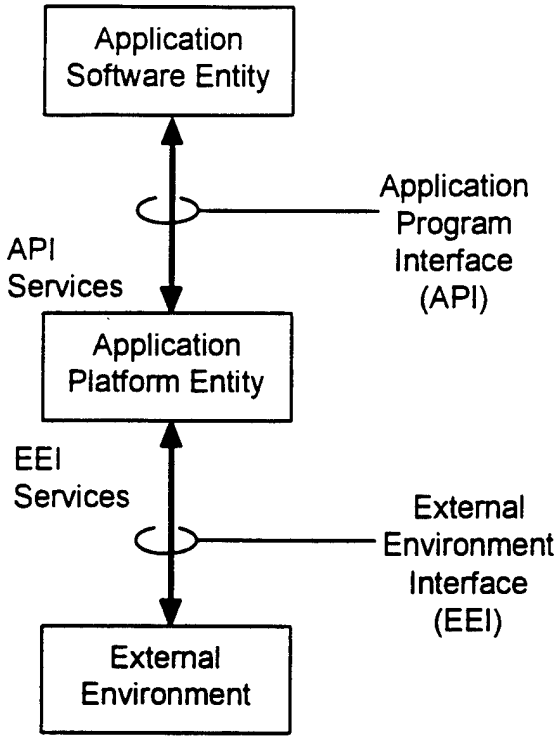
2.3 GENERIC DOD TECHNICAL REFERENCE MODEL

The generic DoD Technical Reference Model is a set of concepts, entities, interfaces, and diagrams that provides a basis for the specification of standards. To a large extent, the Technical Reference Model adopts the foundation work of the IEEE POSIX P1003.0 Working Group as reflected in their Draft Guide to the POSIX Open System Environment (POSIX.0). The POSIX Guide has reached a degree of maturity such that it is undergoing the IEEE balloting process to be sanctioned as an official IEEE document. Within the guide, an interface is defined as "a shared boundary between the two functional units." The functional units are referred to as "entities" when discussing the classification of items related to application portability.

The basic elements of the generic DoD Technical Reference Model are those identified in the POSIX Open System Reference Model and are presented in Figure 2-1. As shown in the figure, the model includes three classes of entities and two types of interfaces as follows:

- Application Software Entity
- Application Program Interface (API)
- Application Platform Entity
- External Environment Interface (EEI)
- External Environment.

This model has been generalized to such a degree that it can accommodate a wide variety of general and special purpose systems. More detailed information is presented in subsequent sections; however, the service specifications allow for subsets or extensions as needed.



Reference: IEEE Draft Guide to the POSIX Open System Environment, June 1992

Figure 2-1. Generic DoD Technical Reference Model

From the perspective of the application software entity, these services are provided by an application platform whether the particular services are provided from the local platform or from remote platforms that may comprise one or more nodes of a larger distributed system. Volume 3 of the TAFIM explains how this generic model can be applied in a distributed environment.

2.3.1 Application Software Entity

In the past, custom systems were developed for specific hardware platforms using proprietary systems software (e.g., operating system, text editor, file management utilities). Such customization was necessary because Government requirements were often more localized than those of the commercial marketplace. These systems were not designed to interoperate with other systems nor to be portable to other hardware platforms. In addition, different systems were developed to perform similar functions at different levels of the overall DoD organization (national, theater, and unit) and for the different Services, (Army, Navy, Air Force, Marine Corps). As a result, many of the systems that were developed included functions redundant with those of other applications. This situation often hindered systems evolution toward greater interoperability, data sharing, portability, and software reuse.

The Technical Reference Model promotes the goals of developing modular applications and promoting software reuse to support the broad range of activities that are integral to any organization. To satisfy these goals, functional (mission-area) applications development will, in many respects, become an integration activity as much as a development activity. Application

development will likely be accomplished by dividing and/or consolidating common functional requirements into discrete modules. Previously developed reusable code or Government-off-the-shelf (GOTS) applications that could satisfy some, if not all, of the new functional requirements would be identified. Such reusable code/applications would then be integrated, to the extent possible, to become the software pieces necessary to complete the mission and/or support applications that will satisfy all of the requirements.

In the Technical Reference Model, applications are divided into mission area applications and support applications. A common set of support applications forms the basis for the development of mission-area applications. Mission-area applications should be designed and developed to access this set of common support applications. As explained in Volume 3, APIs are also used to define the interfaces between mission-area applications and support applications.

The *DoD Goal Security Architecture* (DGSA) in Volume 6 also anticipates the expanding use of NDI products in information system implementations. For this reason, two categories of software are identified, trusted and untrusted. Both categories may have been acquired for an information system implementation as NDI products. However, the trusted software will have been evaluated in accordance with criteria established by responsible agencies for information system security and will need to be maintained under strict configuration management control. Trusted software will mediate the access of all untrusted software to information system resources. Such control, which the DGSA suggests should be in the operating system kernel, will provide the necessary security protection by maintaining separation among applications at different security levels that are simultaneously processing.

2.3.2 Application Program Interface

The API is defined as the interface between the application software and the application platform across which all services are provided. It is defined primarily in support of application portability, but system and application software interoperability also are supported via the communication services API and the information services API. The API specifies a complete interface between the application and the underlying application platform and may be divided into the following groups:

- System Services API (including APIs for Software Engineering Services and Operating System Services)
- Communications Services API (including APIs for Network Services)
- Information Services API (including APIs for Data Management Services and Data Interchange Services)
- Human/Computer Interaction Services API (including APIs for User Interface Services and Graphics Services).

The first API group, System Services, is required to provide access to services associated with the application platform internal resources. The last three API groups (Communications

Services, Information Services, and Human/Computer Interaction Services) are required to provide the application software with access to services associated with each of the external environment entities. APIs for services that cut across the areas are included among all groups where applicable.

A standardized API should be used for accessing security mechanisms. The use of the operating system kernel for maintaining separation among processes executing at different security levels means that this API would be included in the System Services API category above. Such an API will promote independence of security services and security mechanisms, offering transparency to users and applications. This independence will allow different security mechanisms to be accommodated at various stages in an information system life cycle.

2.3.3 Application Platform Entity

The Application Platform is defined as the set of resources that support the services on which application software will execute. It provides services at its interfaces that, as much as possible, make the implementation-specific characteristics of the platform transparent to the application software.

To assure system integrity and consistency, application software entities competing for application platform resources must access all resources via service requests across the API. Examples of application platform services may include an operating system kernel, a realtime monitor program, and all hardware and peripheral drivers.

The application platform concept does not imply or constrain any specific implementation beyond the basic requirement to supply services at the interfaces. For example, the platform might be a single processor shared by a group of applications, a multiprocessor at a single node, or it might be a large distributed system with each application dedicated to a single processor.

The application platform implementations that use the Technical Reference Model may differ greatly depending upon the requirements of the system and its intended use. It is expected that application platforms defined to be consistent with the Technical Reference Model will not necessarily provide all the features discussed here, but will use tailored subsets for a particular set of application software.

2.3.4 External Environment Interface

The External Environment Interface (EEI) is the interface between the application platform and the external environment across which information is exchanged. It is defined primarily in support of system and application software interoperability. User and data portability are directly provided by the EEI, but application software portability also is indirectly supported by reference to common concepts linking specifications at both API and EEI. The EEI specifies a complete interface between the application platform and the underlying external environment, and may be divided into the following groups:

- Human/Computer Interaction Services EEI

- Information Services EEI
- Communications Services EEI.

The Human/Computer Interaction (HCI) Services EEI is the boundary across which physical interaction between the human being and the application platform takes place. Examples of this type of interface include CRT displays, keyboards, mice, and audio input/output devices. Standardization at this interface will allow users to access the services of compliant systems without costly retraining.

The Information Services EEI defines a boundary across which external, persistent storage service is provided, where only the format and syntax are required to be specified for data portability and interoperability.

The Communications Services EEI provides access to services for interaction between application software entities and entities external to the application platform, such as application software entities on other application platforms, external data transport facilities, and devices. The services provided are those where protocol state, syntax, and format all must be standardized for application interoperability.

Security mechanisms to provide for security services in EEIs will be implemented similarly to those required for communications among distributed platforms. That is, the EEIs facilitate communications among distributed platforms. Such implementations will occur primarily in the cross-platform service areas of security and system management. See Sections 2.4.4.2 and 2.4.4.3.

2.3.5 External Environment

The External Environment contains the external entities with which the application platform exchanges information. These entities are classified into the general categories of human users, information interchange entities, and communications entities. Human users are not further classified, but are treated as an abstract, or average person. Information interchange entities include, for example, removable disk packs and floppy disks. Communications entities include telephone lines, local area networks, cabling, and packet switching equipment.

Doctrinal mechanisms (physical, administrative, and personnel) will provide for required security protection of information system components in the external environment.

2.4 DETAILED DOD TECHNICAL REFERENCE MODEL

Figure 2-2 expands upon Figure 2-1 to present the DoD Technical Reference Model entities and interfaces, including the service areas of the Application Platform and related services. Figure 2-2 only depicts entities, interfaces, and service areas and does not imply interrelationships among the service areas.

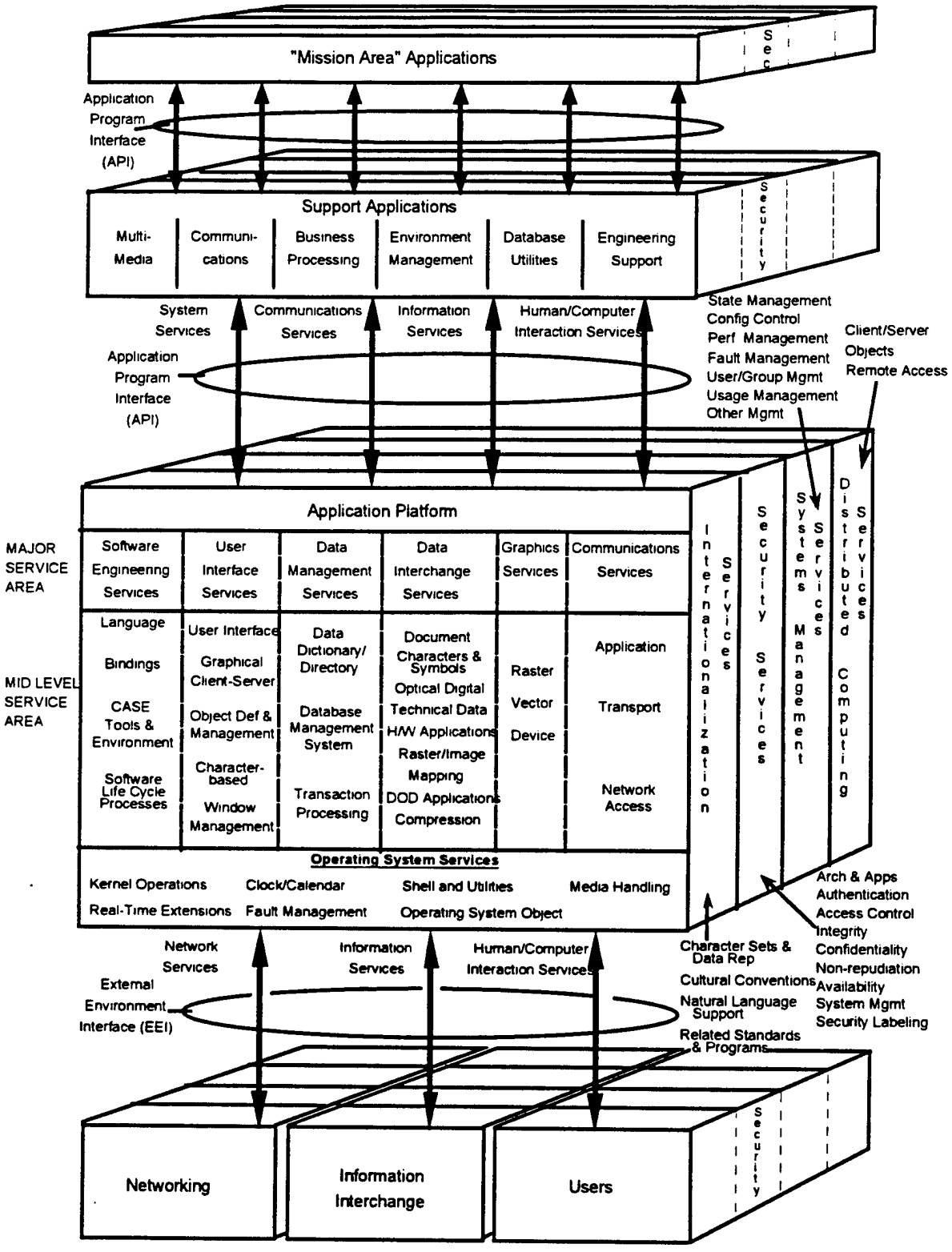


Figure 2-2. Detailed DoD Technical Reference Model

Users should assess their own requirements and create a profile of services, interfaces, and standards that satisfy their own mission-area needs. Users who have adopted earlier versions of the figure should consider adopting the new version of the figure only when planning a major revision of their documentation.

2.4.1 Mission Area Applications

Mission area applications implement specific end-user requirements or needs (e.g., payroll, accounting, materiel management, personnel, control of real-time systems, analysis of order of battle). This application software may be COTS or GOTS, custom developed, or a combination of these. In addition to application software, an information system includes data that can be application specific (e.g., a log of invoices and payments) or an integral part of the software (e.g., application parameters, screen definitions, diagnostic messages). Information systems also include training (e.g., tutorials and on-line help), support tools (e.g., programs for software development, self-test diagnostics), and system management aids (e.g., system administration).

2.4.2 Support Applications

Support applications are common applications (e.g., E-mail, word processing, spreadsheets) that can be standardized across individual or multiple mission areas. The services they provide can be used to develop mission-area-specific applications or can be made available to the user. Support applications may be COTS products selected to provide a service in a common manner, or they may be GOTS applications developed to meet a DoD-unique need and reused in multiple information systems. The Defense Information Infrastructure (DII) Common Operating Environment (COE) includes several support applications to provide common functions such as message handling, network browsing, and mapping. For example, the Joint Mapping Toolkit (JMTK) provides objects and services to support geospatial analysis, mapping (visual) display, geospatial database management, and image preprocessing.

The set of services described in this section provides initial capabilities that will be used to define, acquire, and develop common, shared applications. The services have been grouped into categories by function. The categories and list of services will most likely change over time. New services will be added, or in some cases, existing services will be rearranged and merged into new categories. Some of the services, particularly those found in the multimedia category, will be used as building blocks to implement other services. An implementation of a support application may actually merge several services from several different categories.

The combination of support applications with the services of the platform layer provides the basis for a "common operating environment" to support mission applications. The DII COE implements this concept with a precisely defined client/server architecture for how system components fit together; a standard extensible run-time operating environment that includes "look and feel" operating system and windowing environment standards; a clearly defined set of already implemented, reusable functions; and a collection of APIs for accessing COE components.

2.4.2.1 Multimedia

Multimedia services provide the capability to manipulate and manage information consisting of text, graphics, images, video, and audio. These services can be used directly by mission area applications, but, they can also be used by other support applications to satisfy a common requirement. Multimedia services include:

- **Text processing** services, including the capability to create, edit, merge, and format text.
- **Document processing** services, including the capability to create, edit, merge, and format documents. These services enable the composition of documents that incorporate graphics, images, and even voice annotation, along with stylized text. Included are advanced formatting and editing services such as style guides, spell checking, use of multiple columns, table of contents generation, headers and footers, outlining tools, and support for scanning images into bit-mapped formats.
- **Electronic publishing** services, including incorporation of photographic quality images and color graphics, and advanced formatting and style features such as wrapping text around graphic objects or pictures and kerning (i.e., changing the spacing between text characters). These services also interface with sophisticated printing and production equipment.
- **Geographic information system (GIS)** services, including the capability to create, combine, manipulate, analyze, and present geospatial information. This includes the creation of entity symbology that overlays the map background display and access to standard symbol libraries.
- **Image processing** services providing for the capture, scan, creation, and edit of images in accordance with recognized image formatting standards.
- **Video processing** services, including the capability to capture, compose, and edit video information. Still graphics and title generation services are also provided.
- **Audio processing** services, including the capability to capture, compose, and edit audio information.
- **Multimedia processing** services, including the capability to compress, store, retrieve, modify, sort, search, and print all or any combination of the above-mentioned media, and to perform these actions on two or more types of media simultaneously. This includes support for microform media, optical storage technology that allows for storage of scanned or computer produced documents using digital storage techniques, a scanning capability, and data compression. Additionally, multimedia processing includes hypermedia processing. Hypermedia provides the capability to create and browse documents that allow users to interactively navigate through the document using information embedded in the document.

2.4.2.2 Communications

Communications services provide the capability to send, receive, forward, and manage electronic and voice messages. They also provide real-time information exchange services in support of interpersonal conferences. These services include:

- **Personal messaging** services, including the capability to send, receive, forward, store, display, and manage personal messages. This includes the capability to append files and documents to messages. Messages may include any combination of data, text, audio, graphics, and images and should be capable of being formatted into standard data interchange formats. This service includes the use of directories and distribution lists for routing information, the ability to assign priorities, the use of pre-formatted electronic forms, and the capability to trace the status of messages. Associated services include a summarized listing of incoming messages, a log of messages received and read, the ability to file or print messages, and the ability to reply to or forward messages.

- **Organizational messaging** services, including the capability to send, receive, forward, display, retrieve, prioritize, and manage predefined and unformatted organizational messages. Organizational messages should use standard data interchange formats and may include any combination of data, text, audio, graphics, and images. This includes the capability to review and authenticate messages. Incoming message processing services include receipt, validation, distribution, and dissemination of incoming unformatted messages based on message profiling, message precedence, and system security restrictions. User support services include the selection and display of messages from a message queue, on-line management of search profiles, search and retrieval of stored messages based on message content comparison to queries formulated by the analysts, and composition of record messages for transmission. Outgoing message processing services include coordination by the command's staff organizations, authorized release, and verification of record messages prior to transmission.

- **Enhanced telephony** services, including call forwarding, call waiting, programmed directories, teleconferencing, automatic call distribution (useful for busy customer service areas), call detail recording, and voice mail.

- **Shared screen teleconferencing** services that allow two or more users to communicate and collaborate using audio teleconferencing with common "shared" workstation windows that refresh whenever someone displays new material or changes an existing display. Every user is provided the capability to graphically annotate or modify the shared conference window.

- **Video teleconferencing** services that provide two-way video transmission between different sites. These services include full motion display of events and participants in a bi-directional manner, support for the management of directing the cameras, ranging from fixed position, to sender directed, to receiver directed, to automated sound pickup.

- **Broadcast** services that provide one-way audio or audio/video communications services between a sending location and multiple receiving locations.

- **Computer conferencing** services that allow groups to participate in conferences via computer workstations. These conferences may not occur in real time. Conferees or invited guests can drop in or out of conferences or subconferences at will. The ability to trace the exchanges is provided. Services include exchange of documents, conference management, recording facilities, and search and retrieval capabilities.

2.4.2.3 Business Processing

Business support services provide common office functions used in day-to-day operations. Business support services include:

- **Spreadsheet** services, including the capability to create, manipulate, and present information in tables or charts. This capability should include fourth-generation-language-like capabilities that enable the use of programming logic within spreadsheets.

- **Project management** services, including tools that support the planning, administration, and management of projects.

- **Calculation** services, including the capability to perform routine and complex arithmetic calculations.

- **Calendar** services, including the capability to manage personal tasks and time and to coordinate multiple personal schedules via an automated calendar.

2.4.2.4 Environment Management

This type of service is broader in scope than the other categories in that it exists primarily to manage a particular data processing and/or communications environment. Environment management services integrate and manage the execution of platform services for particular applications and users. These services are invoked via an easy-to-use, high-level interface that enables users and applications to invoke platform services without having to know the details of the technical environment. The environment management service determines which platform service is used to satisfy the request and manages access to it through the API.

- **Batch processing** services support the capability to queue work (jobs) and manage the sequencing of processing based on job control commands and lists of data. These services also include support for the management of the output of batch processing, which frequently includes updated files or databases and information products such as printed reports or electronic documents. Batch processing is performed asynchronously from the user requesting the job.

- **Transaction processing** services provide support for the on-line capture and processing of information in an interactive exchange with the user. This typically involves predetermined sequences of data entry, validation, display, and update or inquiry against a file or database. It also includes services to prioritize and track transactions. Transaction processing services

may include support for distribution of transactions to a combination of local and remote processors.

- **Information presentation and distribution** services are used to manage the distribution and presentation of information from batch and interactive applications. These services are used to shield mission-area applications from how information is used. They allow mission area applications to create generic pools of information without embedding controls that dictate the use of that information. Information distribution and presentation services include the selection of the appropriate formatting services required to accomplish the distribution and presentation of information to a variety of mission-area applications, support applications, and users. It also includes the capability to store, archive, prioritize, restrict, and recreate information.

- **Computer-based training** services provide for integrated training environment on user workstations. Training is available on an as-needed basis for any application available in the environment. Electronic messages are provided at the stroke of a key from anywhere within the application. This includes tutorial training on the application in use and the availability of off-line, on-site interactive training. The DoD on-line training environment will provide in-depth training to the new user, guidance to the novice user, and refresher material for the more experienced user. Computer-based training includes on-line documentation services. As a system service, generalized Help Files that have index, contents, and context-sensitive definitions must be added to all applications. The goal is for a user, through a system-managed activity, to be able to obtain help at any point, while on line.

2.4.2.5 Database Utilities

Database utility services provide the capability to retrieve, organize, and manipulate data extracted from a database management system. These common services provide a consistent interface to the user while providing access to a variety of databases. Database utility services include:

- **Query processing** services that provide for interactive selection, extraction, and formatting of stored information from files and databases. Query processing services are invoked via user-oriented languages and tools (often referred to as fourth-generation languages), which simplify the definition of searching criteria and aid in creating effective presentation of the retrieved information (including use of graphics). Fourth-generation languages are generally all proprietary. Some are in the public domain (for example, Dbase clones are generally referred to as "Xbase" systems), but these all started as proprietary systems. As yet, no public domain fourth-generation language is in wide business use.

- **Screen generation** services that provide the capability to define and generate screens that support the retrieval, presentation, and update of data.

- **Report generation** services that provide the capability to define and generate hardcopy reports composed of data extracted from a database.

- **Networking/concurrent access services** that manage concurrent user access to database management system (DBMS) services.

2.4.2.6 Engineering Support

Engineering support services include support for analysis, design, modeling, development, and simulation for a wide variety of users and environments. This includes computer-aided design services for designing, drafting, and producing engineering drawings. It also includes services provided by decision support development tools and expert system shells.

- **Computer-aided design (CAD)** services provide high-precision drawing tools and modeling capabilities to allow production of engineering specification drawings and other precise drawings.

- **Decision support** services provide interactive modeling and simulation tools that support analysis of alternative decisions.

- **Expert system** services provide artificial intelligence capabilities usually based on knowledge- or rules-based inference engines that recommend or take actions based on presented situations and prior "experiences."

- **Modeling and simulation** services provide the capability to capture or set object characteristics or attributes and parameters of a system of objects, and to portray the relationships and interactions of the objects to assist in the analysis of the system.

2.4.3 Application Platform Service Areas

This section provides a characterization of the terms used to describe the Application Platform Service Areas of the Technical Reference Model (TRM). These terms provide a common definition for the services and interfaces used by DoD information systems and apply to all volumes of the TAFIM. The TAFIM describes the information technology (IT) services provided by the Application Platform Service Area in three levels of detail: Major Service Area, Mid-Level Service Area, and Base Service Area.

Each major heading (MSA) establishes a grouping of services or functionality defined by industry standards and is expressed in a way to be consistent with the manner in which the standards bodies are addressing these groups. The sub-headings, (MLSA and BSA) identify more specific, concrete examples of the functionality represented by the major grouping.

The functionality described by the MSAs, MLSAs, and BSAs defines the services available from the Application Platform across the platform interfaces (APIs and EEIs). The MSAs and MLSAs are identified in the Application Platform Service Area of the TRM, while the BSAs are addressed in Volume 7.

Major Service Area: The Major Service Area category is the highest level of IT functionality. MSAs provide the overall set of standard services that support the objectives of application

portability and system interoperability. The MSAs include Software Engineering Services, User Interface Services, Data Management Services, Data Interchange Services, Graphics Services, and Network Services.

Mid-Level Service Area: MSAs are divided into areas, called Mid-Level Service Areas, that provide like functionality and further decompose the IT functionality. This decomposition is intended to provide a more precise description of each MSA. The MLSAs are represented under the MSAs in bold. The number of categories in each MLSA varies, depending on the variation and complexity of the functionality included in the MSA. The MSAs and MLSAs are fully described in the following sections, 2.4.3.1 through 2.4.3.7.

Base Service Area: The BSA is the next level of granularity below the Mid-Level Service Area and provides the most precise description of IT functionality in a Major Service Area. The BSAs further decompose the IT functionality in each MLSA category. The number of BSAs for any MLSA will vary depending on the complexity of the functionality covered by the MLSA category. The BSAs are fully described in the Information Technology Standards Guidance (ITSG), which supports the development of Volume 7.

2.4.3.1 Software Engineering Services

Professional system developers require tools appropriate to the development and maintenance of applications. These capabilities are provided by software engineering services, which include:

- **Language** services provide the basic syntax and semantic definition for use by a software developer to describe the desired application software function. Shell and executive script language services enable the use of operating system commands or utilities rather than a programming language. Shells and executive scripts are typically interpreted rather than compiled, but some operating systems support compilers for executive scripts. Other programming tools may use procedural or object-oriented languages to define the functionality of the desired applications. Third-generation languages provide primarily command line interfaces and text-based code for defining the applications, while more recent fourth-generation languages are forms-based and provide a graphical interface.

- **Bindings** and object code linking provide the ability for programs to access the underlying application and operating system platform through APIs that have been defined independently of the computer language. They are used by programmers to gain access to these services using methods consistent with the operating system and specific language

  used. Only Ada refers to such actions as "language bindings." All other compilers, DBMSs, and system software refer to such actions as "linking." Linking is operating system dependent, but language independent.

- **Computer-Aided Software Engineering (CASE) tools and environment** include systems and programs that assist in the automated development and maintenance of software. These include, but are not limited to, tools for requirements specification and analysis, for design work and analysis, for creating and testing program code, for documenting, for prototyping, and for group communication. The interfaces among these tools include services for storing and retrieving information about systems and exchanging this information among the various components of the system development environment. An adjunct to these capabilities is the ability to manage and control the configuration of software components, test data, and libraries. Other fourth-generation language tools include software development tools such as artificial intelligence tools and the UNIX command "imake."

- **Software life cycle processes** identify distinct phases in the software life cycle, which is the period of time that begins when a software product is conceptualized and ends when the software is no longer available for use. It includes a set of activities, methods, practices, and transformations that people use to develop and maintain software and the associated products (e.g., project plans, design documents, code, test cases, and user manuals). The software life cycle typically includes a concept phase, requirements phase, design phase, implementation phase, test phase, installation and checkout phase, operation and maintenance phase, and the retirement phase.

2.4.3.2 User Interface Services

User interface services define how users may interact with an application. Depending on the capabilities required by users and the applications, these interfaces may include the following specifications:

- **User interface** services define how users may interact with an application. They provide a consistent way for people who develop, administer, and use a system to gain access to applications programs, operating systems, and various system utilities. The user interface is a combination of menus, screen design, keyboard commands, command language, and help screens, which create the way a user interacts with a computer. The use of mice, touch screens, and other input hardware are included as part of the user interface.

- **Graphical client-server operations** define the relationships between client and server processes operating within a network, in particular, graphical user interface display processes. In this case, the program that controls each display unit is a server process, while independent user programs are client processes that request display services from the server.

- **Object definition and management** services define characteristics of display elements such as color, shape, size, movement, graphics context, user preferences, and interactions among display elements.

- **Character-based user interface** can be either a command-line interface or a menu-driven interface similar to a graphical user interface, but it does not use graphics and may depend solely on the keyboard for user input, i.e., not make use of an explicit pointing device.

Modern systems and applications are and will continue to be based upon graphical user interfaces and the associated standards for such systems. However, many legacy systems still include a large number of character-based terminals and interfaces.

- **Window management** specifications that define how windows are created, moved, stored, retrieved, removed, and related to each other.

User interfaces are often the most complex part of system development and maintenance. Volume 8, the *DoD Human-Computer Interface (HCI) Style Guide*, provides a common framework to document and define functional goals, objectives and requirements, and provides guidance to assist DoD application designers in implementing HCI style standards. Within the past few years, significant advances have been made in user interfaces, both in ease of use and in reducing the development effort required. Although other technologies can be used, most users think of a user interface in terms of a graphical user interface (GUI). A GUI allows a user to specify actions by dragging and dropping or pointing and clicking on an icon that is a pictorial metaphor for the object being acted upon. A GUI can also depict several actions simultaneously by presenting multiple windows.

The services associated with a windows system include the visual display of information on a screen that contains one or more windows or panels, support for pointing to an object on the screen using a pointing device such as a mouse or touch-screen, and the manipulation of a set of objects on the screen through the pointing device or through keyboard entry.

2.4.3.3 Data Management Services

Central to most systems is the management of data that can be defined independently of the processes that create or use it, maintained indefinitely, and shared among many processes. Data management services include:

- **Data dictionary/directory** services allow data administrators and information engineers to access and modify data about data (i.e., metadata). Such data may include internal and external formats, integrity and security rules, and location within a distributed system. Data dictionary/directory services also allow end users/applications to define and obtain data that are available in the database. Data administration defines the standardization and registration of individual data element types to meet the requirements for data sharing and interoperability among information systems throughout the enterprise. Data administration functions include procedures, guidelines, and methods for effective data planning, analysis, standards, modeling, configuration management, storage, retrieval, protection, validation, and documentation.

- **Database management system** services provide data administration, managed objects functionality, and controlled access to and modification of structured data. To manage the data, the DBMS provides concurrency control and facilities to combine data from different schemas. Facilities may also include the capability to manage data in a distributed computing environment where data is stored on multiple, heterogeneous platforms. DBMS

services are accessible through a programming language interface, an interactive data manipulation language interface such as SQL, or an interactive/fourth-generation language interface. For efficiency, database management systems generally provide specific services to create, populate, move, backup, restore/recover, and archive databases, although some of these services could be provided by general file management capabilities described in operating system services.

- **Transaction processing** services support the definition and processing of "transactions." A transaction is a "unit of work" consisting of a series of operations that must be completed together. A transaction is characterized by the ACID properties:

  - Atomicity: implies that the operations of work are either all performed, or none of them are performed

  - Consistency: implies that the operations of a unit of work, if performed at all, are performed accurately, correctly, and with validity, with respect to applications semantics

  - Isolation: implies that the partial results of a unit of work are not accessible, except by operations which are part of the unit of work, and also implies that units of work which share bound data can be serialized

  - Durability: implies that all the effects of a completed unit of work are not altered by any sort of failure. While transaction processing is often associated with database management, it is also applicable in operating systems and communications, as well as physical actions (e.g., dispensing money at a cash machine) that are unrelated to database management.

2.4.3.4 Data Interchange Services

Data interchange services provide specialized support for the interchange of information between applications and to/from the external environment. These services are designed to handle data interchange between applications on the same platform and applications on different (heterogeneous) platforms.

- **Document interchange** services are supported by specifications for encoding the data (e.g., text, pictures, numerics, special characters) and both the logical and visual structures of electronic documents. Services support document exchange between heterogeneous computer systems, exchange of military formatted messages, and electronic forms interchange.

- **Characters and symbols** services provide for interchange of character sets and fonts and standardized date and time representation.

- **Optical digital technologies** (ODT) represents technologies that use the reflective properties of light and an optical recording surface to capture, encode, decode, and store data. ODT predominantly encompasses optical media, optical drives, and scanners.

- **Technical data interchange** services provide facilities for the exchange of technical data. This includes standards for the interchange of graphics data, typically vector graphics, technical specifications, and product data. Product data encompasses technical drawings, documentation, and other data required for product design and manufacturing, including geometric and nongeometric data such as form features, tolerances, material properties, and surfaces.

- **Hardware applications** services provide data interchange services between non-homogeneous hardware components. The most common example of this service is the interchange of information between a computer and a printing device. These services include font information exchange, bar coding, optical disk handling, and graphics device interface (GDI) APIs.

- **Raster/image data interchange** services provide for the handling and manipulation of raster graphics and images. Raster graphics standards are standards for pixel-by-pixel representation of images. Image data standards are standards for the exchange of imagery data, metadata, and attachments to the images.

- **Mapping** services provide formats and facilities for machine-readable mapping, charting, and geospatial data.

- **DoD applications** services are the functional areas unique to DoD missions that are not standardized by nongovernmental standards bodies.

- **Compression** services specify algorithms for compressing data for storage and exchange over a network. Data compression can reduce communications loading by as much as 80 percent without affecting the form of transmitted data. Compression requires application of the same algorithms at the sending and receiving locations. Compression may be used for text and data, still images, and motion images. Compression algorithms for data must be "lossless" so that the expanded output exactly matches the original input. Compression algorithms for still and motion images may be "lossy," where some data may be lost, but the expanded output is not noticeably different from the original input.

2.4.3.5 Graphics Services

Graphics services provide functions required for creating and manipulating pictures. These services include:

- **Raster graphics** represent images as a matrix of dots. Raster graphics images are created by scanners and cameras and are generated by paint software packages. The simplest monochrome bitmap uses one bit (on/off) for each dot. Gray scale bitmaps (monochrome shades) represent each dot with a number large enough to hold all the gray levels. Color

bitmaps require sufficient storage to hold the intensity of red, green, and blue, as would a gray scale equivalent.

- **Vector graphics** represent graphical objects as sets of endpoints for lines, curves, and other geometric shapes with data about width, color, and spaces bounded by lines and curves. The entire image commonly is stored in the computer as a list of vectors called a display list. Vector graphics are used when geometric knowledge about the depicted object is needed. Geometric shapes keep their integrity: a line always can be separately selected, extended, or erased. Today, most screens are raster graphics displays (composed of dots), and the vectors are put into the required dot patterns (rasters) by hardware or software. Vector graphics systems must be supplemented by data interchange standards, such as Initial Graphics Exchange Specification (IGES), Computer Graphics Metafile (CGM), and the Standard for the Exchange of Product Model Data (STEP).

- **Device interfaces** provide API services for accessing graphics devices, such as monitors, scanners, printers, etc.

2.4.3.6 Communications Services

Communications services are provided to support distributed applications requiring data access and applications interoperability in heterogeneous or homogeneous networked environments.

- **Application** services are the functions and interfaces that reside on the underlying network and communications system protocol software and are used by applications. These services are based on the presentation and application layers (layers 6 and 7) of the OSI Reference Model.

- **Transport** services perform a variety of functions concerned primarily with the end-to-end transmission of data across a network and end-to-end reliability. The services performed include end-to-end error detection and recovery, regulating flow control, and managing the quality of service. Transport services correspond to the transport and session layers (layers 4 and 5) of the OSI Reference Model.

- **Subnetwork technologies** services support access to LANs and other networks based on the physical, data link, and network layers (layers 1, 2, and 3) of the OSI Reference Model. This area includes LANs, point-to-point communications, packet switching, circuit switching, and military-unique data communications.

2.4.3.7 Operating System Services

Operating system services are the core services needed to operate and administer the application platform and provide an interface between the application software and the platform. Application programmers will use operating system services to access operating system functions. To separate sensitive data within an information system, the kernel must include mechanisms to control access to that information and to the underlying hardware. Security services are defined in Section 2.4.4.2. Operating system services include:

- **Kernel operations** provide low-level services necessary to create and manage processes, execute programs, define and communicate signals, define and process system clock operations, manage files and directories, and control input/output processing to and from peripheral devices. Thread services provide an underlying service used for multiple concurrent executions within a single computer process. They are designed to allow independent operation and are essential for functions such as multiple process communications.

- **Real-time extension** services support event-driven processes supporting management and actuation of physical processes. For this reason, they are often referred to as sensor-based systems. They are designed to handle and process interrupts from a variety of sources (typically involving some kind of sensor device or timer), process associated information through some type of capture or control algorithm, and respond, if necessary, with an appropriate signal to a control or actuation device.

- **Clock/calendar** services provide mechanisms for measuring the passage of time and maintaining the system time. This includes clocks and timers, real time timers, and distributed timing services.

- **Fault management** includes the prevention, isolation, notification, diagnosis, and correction of fault conditions, which arise whenever a malfunction or abnormal behavior results or may result in an error, outage, or degradation of services. Fault management services allow a system to react to the loss or incorrect operation of system components, and they encompass services for fault detection, isolation, diagnosis, recovery, and avoidance.

- **Shell and utilities** include mechanisms for services at the operator level, such as comparing, printing, and displaying file contents; editing files; searching patterns; evaluating expressions; logging messages; moving files between directories; sorting data; executing command scripts; scheduling signal execution processes; and accessing environment information.

- **Operating system object** services define the rules for creating, deleting, and managing objects.

- **Media handling** services provide for disk and tape formatting for data and interchange of data with applications.

2.4.4 Application Platform Cross-Area Services

Besides the service areas delineated by functional category as presented in Section 2.4.3, another category of services and requirements affects the basic information system architectures within the DoD. Treated in a manner similar to those in POSIX.0, these services are referred to as cross-area services and have a direct effect on the operation of one or more of the functional service areas. In some cases, the cross-area services affect each of the functional service areas in a similar fashion, while in other cases, the cross-area service has an influence that is unique to that particular service area. The discussion of the cross-area services is consolidated here in a

single location within this document in order to provide a coherent perspective when addressing that service.

The cross-area services presently identified and addressed in this section include internationalization, security, system management, and distributed computing. As the reference model evolves, the cross-area services category will be reexamined for additional components or for reallocation into a functional service area of its own.

2.4.4.1 Internationalization Services

As a practice, information system developers have generally designed and developed systems to satisfy a focused set of requirements that are relevant to a specific market segment. That specific market segment may be a nation or a particular cultural market. To make that information system viable, or marketable, to a different segment of the market, a full re-engineering process was usually required. Users or organizations that needed to operate in a multinational or multicultural environment typically did so with multiple, generally incompatible information processing systems. NATO is an example where a number of countries come together to work toward a common goal yet must deal with a diversity of languages and cultures in their day-to-day operations.

Within the context of the TRM, internationalization provides a set of services and interfaces that allow a user to define, select, and change between different culturally related application environments supported by the particular implementation.

- **Character sets and data representation** services include the capability to input, store, manipulate, retrieve, communicate, and present data independently of the coding scheme used. This includes the capability to maintain and access a central character-set repository of all coded character sets and special graphical symbology used throughout the platform, including the appropriate modifications of GUI screens to match character set conventions. Character sets will be uniquely identified so that the end user or application can select the coded character set to be used. This system-independent representation supports the transfer (or sharing) of the values and syntax, but not the semantics, of data records between communicating systems. The specifications are independent of the internal record and field representations of the communicating systems. Also included is the capability to recognize the coded character set of data entities and subsequently to input, communicate, and present that data.

- **Cultural convention** services provide the capability to store and access rules and conventions for cultural entities maintained in a cultural convention repository. These repositories should be available to all applications and be capable of being sorted based upon local rules defined in the repository.

- **Native language support** services provide the capability to support more than one language simultaneously. Messages, menus, forms, and on-line documentation would be displayed in

the language selected by the user. Input from keyboards that have been modified locally to support the local character sets would be correctly interpreted.

- **Related standards and programs** - TBD

2.4.4.2 Security Services

Different groups of individuals within and across the various DoD mission areas need to work with specific sets of data elements. Access to these sets of data elements is to be restricted to authorized users. Satisfaction of this requirement generally has been accomplished by the implementation of separate information systems. Organizations cannot continue to afford to implement separate information systems to satisfy this requirement, nor is it effective to require the user to change interface components every time the need arises to operate with a different restricted data set. Significant benefit will be realized when an individual information system can effectively support the needs of different groups of users and data sets. Such an information system will allow multiple groups to share information systems and data while guaranteeing the separation of data and users as necessary through the use of multi-level security operating systems.

In multi-level security operating systems, the kernel will play the prime role in permitting platforms to handle multiple information domains (security contexts) simultaneously. The separation kernel will be trusted software; that means it will be evaluated in accordance with the requirements stipulated in the documents cited in Volume 7. The separation kernel will mediate all use of the basic information system resources and will provide for strict separation among multiple security contexts by creating separate address spaces for each of them. The separation kernel will provide separation among process spaces by using the protection features of the platform hardware (e.g., processor state registers, memory mapping registers).

The DGSA does not envision security-critical functions being part of these other operating system components. The DGSA envisions such untrusted software performing operations with basic system resources only through invocations of security-critical functions mediated by the separation kernel.

Security services are necessary to protect sensitive information in the information system. The appropriate level of protection is determined based upon the value of the information to the mission-area end users and the perception of threats to it. The information system integrator will need to work with the designated approving authority (DAA) to identify the required level of security protection and acceptable mechanisms for satisfying the requirements. Information system security services are depicted as cross-area services in Figure 2-2 because the mechanisms implemented to provide them may be part of multiple platform service areas. The DGSA currently identifies implementations of security service protection mechanisms in the platform as part of the network and operating system service areas.

The DGSA identifies the following security services that may need to be provided through implementations in information system components. The first five of these services are

consistent with the definitions contained in ISO 7498-2, a standard focusing on security related to open systems interconnection communications. The DGSA extends the ISO 7498-2 definitions to apply to more than communications and identifies availability as a security service.

- **Architectures and applications** provide standards, guidance, and frameworks that help to define security architectures and the placement of security into specific applications and are intended to provide guidance to standards developers. They do not provide implementable specifications against which conformance can be claimed.

- **Authentication** service ensure system entities (processes, systems, and personnel) are uniquely identified and authenticated. The granularity of identification must be sufficient to determine the processes, system, and personnel's access rights. The authentication process must provide an acceptable level of assurance of the professed identity of the entities.

- **Access control** service prevents the unauthorized use of information system resources. This service also prevents the use of a resource in an unauthorized way. This service may be applied to various aspects of access to a resource (e.g., access to communications to the resource, the reading, writing, or deletion of an information/data resource, the execution of a processing resource) or to all accesses to a resource. Security labels are used to manage access and privileges, which are managed for all entities, whether individual users, groups of users, resources, or processes.

- **Integrity** service ensures protection of the system through open system integrity, network integrity, and data integrity. This ensures that data is not altered or destroyed in an unauthorized manner. This service applies to data in permanent data stores and to data in communications messages.

- **Confidentiality** service ensures that data is not made available or disclosed to unauthorized individuals or computer processes through the use of data encryption, security association, and key management. This service will be applied to devices that permit human interaction with the information system. In addition, this service will ensure that observation of usage patterns of communications resources will not be possible.

- **Non-repudiation** services include open systems non-repudiation, electronic signature, and electronic hashing. Non-repudiation services ensure that senders and recipients cannot deny the origin or delivery of data. Non-repudiation mechanisms can be used to validate the source of software packages or to verify that hardware is unchanged from its manufactured state.

- **Availability** service ensures that timely and regular communications services are available. These services are intended to minimize delay or non-delivery of data passed on communications networks. These services include protecting communications networks from accidental or intentional damage and ensuring graceful degradation in communications service.

- **System management** services encompass those security functions required to maintain an operationally secure system. These services include analysis areas such as certification and accreditation and risk management, as well as operationally motivated concerns such as alarm reporting, audit, and cryptographic key management.

- **Security labeling** is the data bound to a resource (which may be a data unit) that names or designates the security attributes of that resource. Security labeling includes security labeling for the following major service areas: user interface, data management, data interchange, graphics, network (data communications), system, and distributed computing.

- **Information system security management** services are concerned with the installation, maintenance, and enforcement of information domain and information system security policy rules in the information system intended to provide these security services. In addition to these core services, security management requires event handling, auditing, and recovery. Standardization of security management functions, data structures, and protocols will enable interoperation of security management application programs (SMAPs) across many platforms in support of distributed security management. Areas for security management standardization are described in Volume 6.

Classes of managed objects for security management are security policies, security services, and security mechanisms. Some information is managed for specific information domains and for the platform in a distributed or non-distributed environment. The items of information that might be included in the security management information base (SMIB) for each information domain and for the platform itself are described in Volume 6.

2.4.4.3 System Management Services

Information systems are composed of a wide variety of diverse resources that must be managed effectively to achieve the goals of an open system environment. While the individual resources (such as printers, software, users, processors) may differ widely, the abstraction of these resources as managed objects allows for treatment in a uniform manner. The basic concepts of management, including operation, administration, and maintenance, may then be applied to the full suite of OSE components along with their attendant services.

Work on systems management services and attendant standards is ongoing. This work is based predominantly on the Open System Interconnection (OSI) network management framework, which applies mainly to networks and the individual nodes on the networks. There is, however, an overlap among certain types of network management functions and individual system management functions. This overlapping area applies equally to networks and individual systems and forms the basis for the OSI approach to systems and network management. Other system management functions in the typical operating system sense are also being addressed and need to be integrated into the overall systems and network management framework. Systems management functionality may be divided according to the management elements that generically apply to all functional resources, which are state management, configuration control, performance management, fault management, user/group management, usage management and other management.

This breakout of system management services parallels the breakout of OSI network management, thereby presenting an overall coherent framework that applies equally to networks

and the individual nodes of the networks. Many of the specific services have no formal standards work in progress; however, industry consortia and others are addressing selected areas.

One important consideration of the standards supporting the services in this area is that they should not enforce specific management policies but rather enable a wide variety of different management policies to be implemented, selected according to the particular needs of the end-user installations.

- **State management** services provide for mechanisms that monitor, maintain, and change the state of the system or components of the system.

- **Configuration control** services address four basic functions: identification, control, status accounting, and verification. Identification involves identifying and specifying all component resources. Control implies the ability to freeze configuration items and then to change them only through a process involving agreement of appropriate name authorities. Status accounting involves the recording and report of all current and historical data about each configuration item. Verification consists of a series of reviews and audits to ensure conformity between the actual configuration item and the information recorded about it. The services which provide these functions include software distribution and license management.

- **Performance management** services allow information technology resources to be managed efficiently. Performance aspects of hardware, software, and network components must be monitored and subsequently made available to the system manager. The manager must then have access to services and parameters with which to tune the system to meet performance targets. This is accomplished through batch scheduling, system resource management, print and storage device management, system startup and shutdown, subsystem management, and communication of management information.

- **Fault management** services allow a system to react to the loss or incorrect operation of system components at various levels (hardware, software, etc.). Fault management involves event management and network error recovery.

- **User/group management** services provide traditional system administration interfaces for administering users and groups. These services are mechanisms for system and network administrators to use when implementing a management policy across a system. Administrators can use the services to establish domains and policies for management throughout the system. They can provide the ability for applications to access group and user databases. Users can set up their own areas of management and policies or use system defaults that are included in management services.

- **Usage management and cost allocation** services include the management of software licensing, system cost management, and system resource allocation. Software license management for a system provides license administration, management, and enforcement services that allow more detailed, firm, and equitable licensing terms for users, and better protection against illegal software usage for vendors. Cost management services provide the ability to cost services for charging and reimbursement and to measure and prioritize resource usage.

System resource allocation allows system administrators to control the amount of system resources available to users.

- **Other management** services include the following services which do not fit cleanly into any other management area: database administration, object-oriented database management, floppy disk formatting and handling, POSIX tape labeling and tape volume processing, and print management. Database and object-oriented database administration provide facilities and interfaces for the management of databases and object-oriented databases, respectively. Floppy disk formatting and handling standards provide formats and interfaces for the exchange, backup, and restoration of data to or from floppy disks. POSIX tape labeling and tape volume processing provide for standardized methods of handling and reading data stored on tape media and containing certain types of administrative information automatically readable by tape-handling software. Print management services are used by management and user applications to send a file to a printer, cancel a print job, and get printer status information. (Security system management services are discussed above, in Section 2.4.4.2, as part of security services.)

System management application processes, using information in the information base, will be used to establish the required security contexts for interactive communications among distributed platforms operating in various information domains simultaneously. This approach is intended to support secure distributed computing services. System management application processes will also be used to provide the security protection of store-and-forward communications in which the requisite security contexts cannot be handled within the message.

2.4.4.4 Distributed Computing Services

Distributed computing services provide specialized support for applications that may be physically or logically dispersed among computer systems in a network yet wish to maintain a cooperative processing environment. The classical definition of a computer becomes blurred as the processes that contribute to information processing become distributed across a facility or a network. As with other cross-cutting services, the requisite components of distributed computing services typically exist within particular service areas. They are described below to offer a coherent view of this important service.

- **Client/server** services provide support for computing services which are partitioned into requesting processes (clients) and providing processes (servers), whether on the same platform or in a distributed environment.

- **Object** services support the definition, instantiation, and interaction of objects in a distributed environment, and include services which handle operating system bindings, message transport and delivery, and data persistence.

- **Remote access** services provide location transparency functionality for distributed computing services, allowing users and client processes to access appropriate systems resources (files, data, processes) without regard to the location of either.

This page intentionally left blank.

APPENDIX A

REFERENCES

Note: References appearing in this section represent documents used in preparation of the TAFIM, including some sources used at the time of initial document development that may no longer be current or applicable. The reader is advised to check the current applicability of a reference appearing in this list before using it as an information source. The reference section will be completely reviewed and revised for the next release of the TAFIM.

1. Executive Level Group for Defense Corporate Information Management, A Plan for Corporate Information Management for the Department of Defense, 11 September 1991.

2. Application Portability Profile (APP), The U.S. Government's Open System Environment Profile OSE/1 Version 2.0, NIST SP-500-210, June 1993.

3. Army Tactical Command and Control Information System, Technical Standards for CCISs, Third Edition, 21 January 1992.

4. AT&T, Open Look Graphical User Interface Trademark Guide, 1990.

5. DEPSECDEF Memo, 14 January 91, Implementation Plan for Corporate Information Management, with Enclosure 774.

6. DIA, DIA Information System Architecture Standards and Products, 10 May 1990.

7. DLA Office of Information Systems and Technology, Information Resources Management Environment Vision and Prescription, Version 1.1, April 1991.

8. DoD Intelligence Information System (DODIIS) Reference Model for the 1990s, Defense Intelligence Agency, Draft, 14 May 91.

9. IEEE Draft Guide to the POSIX Open System Environment (P1003.0/D15), Institute of Electrical and Electronics Engineers, Inc., May 1992.

10. NIST, FIPS 146-2, Profiles for Open Systems Networking Technologies, 1996.

11. NIST Special Report 500-187, Application Portability Profile (APP): The U.S. Government's Open System Environment Profile OSE/1, Version 1.0, May 1991.

12. NIST Special Publication 500-163, Government Open Systems Interconnection Profile (GOSIP) User's Guide, 2nd Edition.

13. NIST Special Publication 500-201, Reference Model for Frameworks of Software Engineering Environments (Technical Report ECMA TR/55, 2nd Edition), December 1991.

14. OSF, OSF/Motif Application Environment Specification User Environment, Volume 1.0, Rev A, 1990.

15. OSF, OSF/Motif Programmer's Guide, Rev 1.0, 1990.

16. OSF, OSF/Motif Style Guide, Rev 1.0, 1990.

17. OSF, OSF/Motif User's Guide, Rev 1.0, 1990.

18. Plan for Implementation of Corporate Information Management in DoD, ASD/C3I, 8 January 1991.

19. SECDEF Memo, November 16, 1990, Implementation of Corporate Information Management Principles w/Enclosure.

20. SM-684-88, Policy and Procedures for Management of Command, Control, and Communications Systems, JCS, undated.

21. Sun Microsystems, Inc., Open Look Graphical User Interface Application Style Guidelines, 1989.

22. Sun Microsystems, Inc., Open Look Graphical User Interface Functional Specifications, 1989.

23. Strategies for Open Systems, Stage Two: The Experience With Open Systems, DMR Group, Inc., Boston, 1990, pp. 196.

24. X/OPEN Company, Ltd., X/OPEN Portability Guide, Version 3 (XPG3), 1988.

25. X/Open Portability Guide, Issue 3, Volumes 1-7, X/Open Company, Ltd., Prentice Hall, Inglewood Cliffs, NJ, 1988.

APPENDIX B

ACRONYMS

AITS	Adopted Information Technology Standards
AMWG	Architecture Methodology Working Group
ANSI	American National Standards Institute
API	Application Program Interface
APP	Application Portability Profile
ASC	Accredited Standards Committee
ASD(C3I)	Assistant Secretary of Defense, Command, Control, Communications, and Intelligence
BSA	Base Service Area
CAD	Computer-Aided Design
CALS	Computer-Aided Acquisition and Logistic Support
CAP	Communication-Electronics Accommodation Program
CASE	Computer-Aided Software Engineering (See ISEE)
CGM	Computer Graphics Metafile
CIM	Corporate Information Management
COTS	Commercial-Off-the-Shelf
DAA	Designated Approving Authority
DBMS	Database Management System
DDI	Director of Defense Information
DEPSECDEF	Deputy Secretary of Defense
DGSA	Defense Goal Security Architecture
DISA	Defense Information Systems Agency
DLA	Defense Logistics Agency
DoD	Department of Defense
DODIIS	DoD Intelligence Information System
DSRS	DoD Software Reuse System
EEI	External Environment Interface
FIPS	Federal Information Processing Standard
GOTS	Government-Off-the-Shelf

GUI	Graphical User Interface
HCI	Human Computer Interface
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IGES	Initial Graphics Exchange Specification
INX	Information Exchange
ISO	International Organization for Standardization
IT	Information Technology
ITPB	Information Technology Policy Board
ITSI BBS	Information Technology Standards Information Bulletin Board System
JIEO	Joint Interoperability and Engineering Organization
JTC	Joint Technical Committee
MSA	Major Service Area
MLSA	Mid-Level Service Area
NATO	North Atlantic Treaty Organization
NDI	Nondevelopmental Item
NIST	National Institute of Standards and Technology
OA&M	Operation, Administration, and Maintenance
ODT	Optical Digital Technologies
OSD	Office of the Secretary of Defense
OSE	Open System Environment
OSF	Open Software Foundation
OSI	Open System Interconnection
POSIX	Portable Operating System Interface (for Computer Environments)
SECDEF	Secretary of Defense
SMAP	Security Management Application Program
SMIB	Security Management Information Base
STEP	Standard for the Exchange of Product Model Data
TRM	Technical Reference Model
UI	UNIX International

APPENDIX C

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE MEMORANDA CONCERNING OPEN SYSTEMS IMPLEMENTATION AND THE TECHNICAL REFERENCE MODEL

This appendix provides the text of a memorandum from the Assistant Secretary of Defense concerning open systems implementation and the Technical Reference Model, dated 30 March 1995.

MEMORANDUM FROM
THE ASSISTANT SECRETARY OF DEFENSE

March 30, 1995

MEMORANDUM FOR
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARY OF THE ARMY (RD&A)
ASSISTANT SECRETARY OF THE NAVY (RD&A)
ASSISTANT SECRETARY OF THE AIR FORCE
(ACQUISITION) (SAF/AQ)
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTOR, JOINT STAFF

SUBJECT: Technical Architecture Framework for Information Management (TAFIM), Version 2.0

My memorandum dated June 23, 1994 established the TAFIM as the single framework to promote the integration of Department of Defense (DoD) information systems, expanding the opportunities for interoperability and enhancing our capability to manage information resources across the Department. The latest version of the TAFIM, Version 2.0, is complete and fully coordinated. Version 2.0 consists of seven volumes as shown in the attachment. The TAFIM will continue to guide and enhance the evolution of the Department's information systems technical architectures.

I want to reiterate two important points that I made in my June 1994 memorandum. First, the Department remains committed to a long range goal of an open systems environment where interoperability and cross functional integration of our systems and portability/reusability of our software are key benefits. Second, the further selection and evaluation of migration systems should take into account this long range goal by striving for conformance to the TAFIM to the extent possible.

Effectively immediately, new DoD information systems development and modernization programs will conform to the TAFIM. Evolutionary changes to migration systems will be governed by conformance to the TAFIM.

The TAFIM is maintained by the Defense Information Systems Agency (DISA) and is available electronically via the DISA On-Line Standards Library. Hardcopy is available through the Defense Technical Information Center. The TAFIM is an evolving set of documents and comments for improving may be provided to DISA at any time. The DISA action officer is Mr. Bobby Zoll, (703) 735-3552. The OSD action officer is Mr. Terry Hagle, (703) 604-1486.

s/Emmett Paige, Jr.

APPENDIX D

PROPOSING CHANGES TO TAFIM VOLUMES

D.1 INTRODUCTION

Changes to the TAFIM will occur through changes to the TAFIM documents (i.e., the TAFIM numbered volumes, the CMP, and the PMP). This appendix provides guidance for submission of proposed TAFIM changes. These proposals should be described as specific wording for line-in/line-out changes to a specific part of a TAFIM document.

Use of a standard format for submitting a change proposal will expedite the processing of changes. The format for submitting change proposals is shown in Section D.2. Guidance on the use of the format is provided in Section D.3.

A Configuration Management contractor is managing the receipt and processing of TAFIM change proposals. The preferred method of proposal receipt is via e-mail in ASCII format, sent via the Internet. If not e-mailed, the proposed change, also in the format shown in Section D.2, and on both paper and floppy disk, should be mailed. As a final option, change proposals may be sent via fax; however, delivery methods that enable electronic capture of change proposals are preferred. Address information for the Configuration Management contractor is shown below.

Internet: **tafim@bah.com**

Mail: **TAFIM**
Booz, Allen & Hamilton Inc.
5201 Leesburg Pike, 4th Floor
Falls Church, VA 22041

Fax: **703/824-3770**; indicate "TAFIM" on cover sheet.

D.2 TAFIM CHANGE PROPOSAL SUBMISSION FORMAT

a. Point of Contact Identification

(1) Name:

(2) Organization and Office Symbol:

(3) Street:

(4) City:

(5) State:

(6) Zip Code:

(7) Area Code and Telephone #:

(8) Area Code and Fax #:

(9) E-mail Address:

b. Document Identification

(1) Volume Number :

(2) Document Title:

(3) Version Number:

(4) Version Date:

c. Proposed Change # 1

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

d. Proposed Change # 2

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

n. Proposed Change # n

(1) Section Number:

(2) Page Number:

(3) Title of Proposed Change:

(4) Wording of Proposed Change:

(5) Rationale for Proposed Change:

(6) Other Comments:

D.3 FORMAT GUIDANCE

The format in Section D.2 should be followed exactly as shown. For example, Page Number should not be entered on the same line as the Section Number. The format can accommodate, for a specific TAFIM document, multiple change proposals for which the same individual is the

Point of Contact (POC). This POC would be the individual the TAFIM project staff could contact on any question regarding the proposed change. The information in the **Point of Contact Identification** part (**D.2 a**) of the format would identify that individual. The information in the **Document Identification** part of the format (**D.2 b**) is self-evident, except that volume number would not apply to the CMP or PMP. The proposed changes would be described in the **Proposed Change #** parts (**D.2 c, D.2 d, or D.2 n**) of the format.

In the **Proposed Change #** parts of the format, the Section number refers to the specific subsection of the document in which the change is to take place (e.g., Section 2.2.3.1). The page number (or numbers, if more than one page is involved) will further identify where in the document the proposed change is to be made. The Title of Proposed Change field is for the submitter to insert a brief title that gives a general indication of the nature of the proposed change. In the Wording of Proposed Change field the submitter will identify the specific words (or sentences) to be deleted and the exact words (or sentences) to be inserted. In this field providing identification of the referenced paragraph, as well as the affected sentence(s) in that paragraph, would be helpful. An example of input for this field would be: "Delete the last sentence of the second paragraph of the section and replace it with the following sentence: 'The working baseline will only be available to the TAFIM project staff.'" The goal is for the commentor to provide proposed wording that is appropriate for insertion into a TAFIM document without editing (i.e., a line-out/line-in change). The D.2 c (5), D.2 d (5), or D.2 n (5) entry in this part of the format is a discussion of the rationale for the change. The rationale may include reference material. Statements such as "industry practice" would carry less weight than specific examples. In addition, to the extent possible, citations from professional publications should be provided. A statement of the impact of the proposed change may also be included with the rationale. Finally, any other information related to improvement of the specific TAFIM document may be provided in D.2 c (6), D.2 d (6), or D.2 n (6) (i.e., the Other Comments field). However, without some degree of specificity these comments may not result in change to the document.

This page intentionally left blank.